

On the Secrecy Capacity Region of Parallel Broadcast Channel with Common and Confidential Messages

Ahmed Benfarah, Stefano Tomasin and Nicola Laurenti
 Department of Information Engineering, University of Padova
 via Gradenigo 6/B, 35131 Padova, Italy. Email: firstname.lastname@dei.unipd.it

Abstract—We consider a broadcast communication system over parallel sub-channels where the transmitter sends a common message to two users, and two confidential messages to each user which need to be kept secret from the other user. Assuming perfect channel state information at the transmitter, the characterization of the boundary for the secrecy capacity region turns into solving a power allocation optimization problem. We derive the power allocation algorithm reaching the boundary of the secrecy capacity region under an average total power constraint. Numerical simulations are presented in comparison to existing power allocation schemes, showing the merit of the proposed algorithm.

Index Terms—Broadcast communication, parallel channel, physical layer security, power allocation.

I. INTRODUCTION

With the widespread adoption of wireless networks, security becomes an inherent issue of nowadays communications. In this context, *physical layer security* arises as a promising tool to enhance security in emerging wireless networks as a complement to traditional security solutions. The basic concepts of physical layer security were founded by the pioneering work of Wyner [1]. He introduced the *wiretap* channel model in which the transmitter aims to send reliably a confidential message to the legitimate receiver in presence of the wiretapper eavesdropper. The information-theoretic performance measure is the *secrecy capacity* defined by the maximum information rate at which the transmitter can reliably communicate secret message to the receiver, without the eavesdropper being able to decode it. Later, the wiretap channel has witnessed a renewed interest and many research works investigated secrecy capacity of wireless fading channels [2], [3], [4] and multiple-input multiple-output (MIMO) channels [5], [6], [7]. All of these works deal with the point-to-point wiretap model. Recently, there has been an effort to generalize physical layer security to the multi-user context (see [8] for a survey).

One important category of multi-user physical layer security scenario is *broadcast channel with confidential messages* (BCC) [9]. In [10], the authors established the secrecy capacity region of parallel sub-channels and fading channels in a scenario where a source node has a common message for two receivers and confidential message intended only for one receiver. Extensive research work was made to characterize the secrecy capacity region of Gaussian MIMO broadcast channels [11], [12], [13], [14]. The communication scenario

considered in all these works consists of a source node communicating with two malicious receiving users eavesdropping each other. Secure broadcasting to multiple receivers was analyzed in [15], [16] when the eavesdropper is external to the group of users. For an overview of the different communication scenarios considered in the literature of BCC, the reader can see [17].

In this paper, we consider a broadcast communication over parallel sub-channels with one transmitter and two users. The system appropriately describes a broadcast orthogonal frequency division multiplexing (OFDM) transmission. The transmitter aims to send three independent messages: one common message to both users and two confidential messages intended for each user. We first characterize the secrecy capacity region for parallel BCC with a common message and two confidential messages. Then, we derive the optimal power allocation algorithm that maximizes the weighted sum-rate of the three messages under a total power constraint. The algorithm allows a complete characterization of the boundary of the secrecy capacity region for this communication scenario. Our contribution generalizes some related work which considered only two out of the three possible messages. In [18], [19], the authors derived the optimal power allocation in presence of two confidential messages without a common while in [10], the optimal power allocation for the case of one common message and one confidential message has been established.

The rest of the paper is organized as follows. Section II provides the system model of the parallel BCC with common message and two confidential messages, and a first characterization of the secrecy capacity region. Then, the optimal power allocation that maximizes the weighted sum-rate is obtained in Section III. Numerical results are provided in Section IV including a comparison with existing approaches, before conclusions are outlined in Section V.

Notation: Vectors and matrices are written in bold letters. We denote the base-2 logarithm by \log . We indicate the positive part of a real quantity x as $[x]^+ = \max\{x; 0\}$. $\mathbb{E}[X]$ denotes the expectation of the random variable X , $I(X; Y)$ denotes the mutual information between variables X and Y . tr denotes the trace of a square matrix.

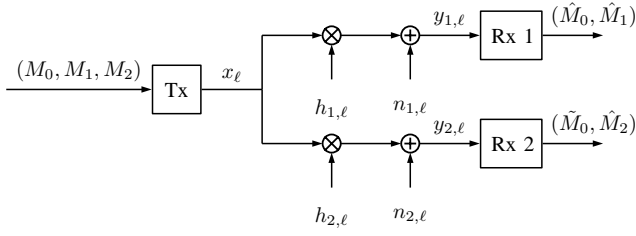


Fig. 1. Model of the parallel channel broadcast communication with common and confidential messages.

II. SYSTEM MODEL

We consider a parallel channel (e.g. OFDM) broadcast communication with L sub-channels, one transmitter and two receiving users. Note that we consider real-valued signals. The transmitter sends real-valued symbol x_ℓ at sub-channel ℓ . The channel input is subject to the average total power constraint

$$\sum_{\ell=1}^L \mathbb{E}\{x_\ell^2\} \leq P. \quad (1)$$

We assume transmission over a quasi-static fading channel; that is the channel remains constant over the entire duration of a single packet. At the two receivers we obtain

$$y_{i,\ell} = h_{i,\ell}x_\ell + n_{i,\ell} \quad (2)$$

where $i=1, 2$ is the receiver index, $n_{i,\ell}$ are real-valued zero-mean unit variance additive white Gaussian noise (AWGN) terms, and $h_{i,\ell}$ are the real-valued channel gains for user i . Noise components for different sub-channels are independent. In addition, we assume that the channel state information (CSI) is known at both the transmitter and the receivers.

As illustrated in Fig. 1, we consider a broadcast communication scenario in which the transmitter aims at transmitting a common message M_0 with information rate R_0 and two separate confidential messages M_1 and M_2 with information rates R_1 and R_2 respectively [20]. The common message M_0 is intended for both receivers, while confidential message M_i is intended for receiver i and needs to be kept secret from the other receiver. The transmitter allocates power $p_{i,\ell}$ on sub-channel ℓ to the confidential message for user i , and power $p_{0,\ell}$ to the common message.

To the aim at having *reliable transmissions* to the intended receiver, i.e., the error probabilities on the messages at the intended receivers must be vanishing as the codeword length n grows to infinity. *Secrecy* is measured in terms of the information leakage to the non-intended receiver [1], [9], i.e., defining $\mathbf{Y}_i^n = [\mathbf{y}_i(1), \dots, \mathbf{y}_i(n)]$, we require

$$\frac{1}{n} \mathbb{I}(M_1; M_0, M_2, \mathbf{Y}_2^n) \rightarrow 0; \quad \frac{1}{n} \mathbb{I}(M_2; M_0, M_1, \mathbf{Y}_1^n) \rightarrow 0, \quad (3)$$

as $n \rightarrow \infty$.

A. Secrecy capacity region

The secrecy capacity region \mathcal{C}_s is defined as the closure of all rate triples (R_0, R_1, R_2) that can be achieved by any coding scheme while maintaining both reliability and secrecy requirements. The secrecy capacity region of this broadcast communication scenario $\mathcal{C}_s(\mathbf{K})$ was characterized in [13], [14] for the general Gaussian MIMO channels under a matrix covariance constraint \mathbf{K} . The secrecy capacity region under the total power constraint \mathcal{C}_s is obtained by the union of the $\mathcal{C}_s(\mathbf{K})$ over all covariance matrices which satisfy $\text{tr}(\mathbf{K}) \leq P$. The parallel channel can be seen as a special case of MIMO channels. Furthermore, it was established in [10] that having independent inputs for each sub-channel is optimal for the parallel BCC. Consequently, it is sufficient to have diagonal input covariance matrices [14], [13] for the parallel broadcast channel. We define the power allocation vector $\mathbf{p} = [p_{0,1}, \dots, p_{0,L}, p_{1,1}, \dots, p_{1,L}, p_{2,1}, \dots, p_{2,L}]$. The set \mathcal{P} includes all power allocation vectors \mathbf{p} that satisfy the total power constraint (1), i.e.,

$$\mathcal{P} = \left\{ \mathbf{p} : \sum_{\ell=1}^L (p_{0,\ell} + p_{1,\ell} + p_{2,\ell}) \leq P \right\}. \quad (4)$$

Let us define sets

$$S_1 = \{\ell : h_{1,\ell}^2 > h_{2,\ell}^2\} \quad \text{and} \quad S_2 = \{\ell : h_{2,\ell}^2 \geq h_{1,\ell}^2\}. \quad (5)$$

Thereby, the secrecy capacity region of the parallel BCC with common and two confidential messages can be written as

$$\mathcal{C}_s = \bigcup_{\mathbf{p} \in \mathcal{P}} \mathcal{R}(\mathbf{p})$$

$$\mathcal{R}(\mathbf{p}) = \begin{cases} (R_0, R_1, R_2) : \\ 0 \leq R_0 \leq R_0^{\max}(\mathbf{p}) = \min\{R_{01}^{\max}(\mathbf{p}), R_{02}^{\max}(\mathbf{p})\} \\ 0 \leq R_i \leq R_i^{\max}(\mathbf{p}) \end{cases}. \quad (6)$$

The terms $R_{01}^{\max}(\mathbf{p})$, $R_{02}^{\max}(\mathbf{p})$, $R_1^{\max}(\mathbf{p})$ and $R_2^{\max}(\mathbf{p})$ are given by

$$R_{01}^{\max}(\mathbf{p}) = \frac{1}{2} \sum_{\ell=1}^L \log(1 + h_{1,\ell}^2[p_{0,\ell} + p_{1,\ell} + p_{2,\ell}]) - \log(1 + h_{2,\ell}^2[p_{1,\ell} + p_{2,\ell}]) \quad (7)$$

$$R_{02}^{\max}(\mathbf{p}) = \frac{1}{2} \sum_{\ell=1}^L \log(1 + h_{2,\ell}^2[p_{0,\ell} + p_{1,\ell} + p_{2,\ell}]) - \log(1 + h_{1,\ell}^2[p_{1,\ell} + p_{2,\ell}]) \quad (8)$$

$$R_1^{\max}(\mathbf{p}) = \frac{1}{2} \sum_{\ell \in S_1} \log(1 + h_{1,\ell}^2 p_{1,\ell}) - \log(1 + h_{2,\ell}^2 p_{1,\ell}) \quad (9)$$

$$R_2^{\max}(\mathbf{p}) = \frac{1}{2} \sum_{\ell \in S_2} \log(1 + h_{2,\ell}^2 p_{2,\ell}) - \log(1 + h_{1,\ell}^2 p_{2,\ell}). \quad (10)$$

The expression of the secrecy capacity region states that the receivers decode first the common message by treating the

confidential messages as noise. Then, each receiver decodes its own confidential message.

The secrecy capacity region given in (6) is convex [10]. Thus, the boundary of the secrecy capacity region can be characterized as follows. For each triplet (R_0^*, R_1^*, R_2^*) on the boundary, there exist $w_0 \geq 0$, $w_1 \geq 0$ and $w_2 \geq 0$ such that (R_0^*, R_1^*, R_2^*) is a solution to an optimization problem. In fact, the power allocation \mathbf{p}^* that achieves the boundary point (R_0^*, R_1^*, R_2^*) is the solution to the following optimization problem

$$\mathbf{p}^* = \arg \max_{\mathbf{p}} [w_0 \min\{R_{01}^{\max}(\mathbf{p}), R_{02}^{\max}(\mathbf{p})\} + w_1 R_{11}^{\max}(\mathbf{p}) + w_2 R_{22}^{\max}(\mathbf{p})] \quad (11a)$$

$$s.t. \quad (4). \quad (11b)$$

The optimization (11) allows a complete characterization of the boundary of the secrecy capacity region and provides the power allocations that achieve this boundary. Our goal is to solve this optimization problem.

III. POWER ALLOCATION ALGORITHM

The optimization problem (11) is a max-min optimization, and can be solved by the method used in [21]. The main idea of the method is stated in the following lemma.

Lemma 1. *The optimal \mathbf{p}^* which solves (11) is solution of one of the following three problems:*

$$(P1) \mathbf{p}^{(1)} = \arg \max_{\mathbf{p} \in \mathcal{P}} [w_0 R_{01}^{\max}(\mathbf{p}) + w_1 R_{11}^{\max}(\mathbf{p}) + w_2 R_{22}^{\max}(\mathbf{p})]$$

$$(P2) \mathbf{p}^{(2)} = \arg \max_{\mathbf{p} \in \mathcal{P}} [w_0 R_{02}^{\max}(\mathbf{p}) + w_1 R_{11}^{\max}(\mathbf{p}) + w_2 R_{22}^{\max}(\mathbf{p})]$$

$$(P3) \mathbf{p}^{(3)} = \arg \max_{\mathbf{p} \in \mathcal{P}} [w_0 (\alpha R_{01}^{\max}(\mathbf{p}) + (1-\alpha) R_{02}^{\max}(\mathbf{p})) + w_1 R_{11}^{\max}(\mathbf{p}) + w_2 R_{22}^{\max}(\mathbf{p})].$$

α is a parameter in $[0; 1]$. In particular,

$$\mathbf{p}^* = \begin{cases} \mathbf{p}^{(1)} & \text{if } R_{01}^{\max}(\mathbf{p}^{(1)}) < R_{02}^{\max}(\mathbf{p}^{(1)}) \\ \mathbf{p}^{(2)} & \text{if } R_{01}^{\max}(\mathbf{p}^{(2)}) > R_{02}^{\max}(\mathbf{p}^{(2)}) \\ \mathbf{p}^{(3)} & \text{if } R_{01}^{\max}(\mathbf{p}^{(3)}) = R_{02}^{\max}(\mathbf{p}^{(3)}) \end{cases} \quad (12)$$

We now focus on the solution of problems (P1)-(P3). Before introducing the result, we define the following terms:

$$\beta_{i,\ell} = \frac{1}{2} \left(\delta_{i,\ell} \left(\delta_{i,\ell} + \frac{2w_i}{\lambda \ln 2} \right) \right)^{1/2} - \frac{1}{2} \left(\frac{1}{h_{2,\ell}^2} + \frac{1}{h_{1,\ell}^2} \right) \quad (13a)$$

$$\gamma_\ell^{(1)} = \frac{w_0}{2\lambda \ln 2} - \frac{1}{h_{1,\ell}^2} \quad (13b)$$

$$\zeta_{i,\ell}^{(1)} = \frac{w_i}{w_0} \delta_{i,\ell} - \frac{1}{h_{2,\ell}^2} \quad (13c)$$

$$\eta_\ell^{(2)} = \frac{w_0}{2\lambda \ln 2} - \frac{1}{h_{2,\ell}^2} \quad (13d)$$

$$\kappa_{i,\ell}^{(2)} = \frac{w_i}{w_0} \delta_{i,\ell} - \frac{1}{h_{1,\ell}^2} \quad (13e)$$

$$\nu_\ell^{(3)} = \frac{1}{2} \left(\left(\delta_{1,\ell} - \frac{w_0}{2\lambda \ln 2} \right)^2 + \frac{2w_0\alpha}{\lambda \ln 2} \delta_{1,\ell} \right)^{1/2} - \frac{1}{2} \left(\frac{1}{h_{2,\ell}^2} + \frac{1}{h_{1,\ell}^2} - \frac{w_0}{2\lambda \ln 2} \right) \quad (13f)$$

$$\xi_{i,\ell}^{(3)} = \frac{w_i}{w_0} \delta_{i,\ell} - \left(\frac{\alpha}{h_{2,\ell}^2} + \frac{1-\alpha}{h_{1,\ell}^2} \right) \quad (13g)$$

where $\delta_{1,\ell} = 1/h_{2,\ell}^2 - 1/h_{1,\ell}^2$, $\delta_{2,\ell} = -\delta_{1,\ell}$, and $\lambda \geq 0$ is a parameter.

Theorem 1. *The solutions of problems (P1)-(P3) are:*

(P1) For $\ell \in S_1$, if $\frac{w_1}{w_0} > \frac{h_{1,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, then

$$p_{0,\ell}^{(1)} = [\gamma_\ell^{(1)} - \zeta_{1,\ell}^{(1)}]^+ \quad \text{and} \quad p_{1,\ell}^{(1)} = [\min\{\beta_{1,\ell}; \zeta_{1,\ell}^{(1)}\}]^+.$$

Otherwise, if $\frac{w_1}{w_0} \leq \frac{h_{1,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, then

$$p_{0,\ell}^{(1)} = [\gamma_\ell^{(1)}]^+ \quad \text{and} \quad p_{1,\ell}^{(1)} = 0.$$

For $\ell \in S_2$, if $\frac{w_2}{w_0} > \frac{h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, then

$$p_{0,\ell}^{(1)} = [\gamma_\ell^{(1)} - \zeta_{2,\ell}^{(1)}]^+ \quad \text{and} \quad p_{2,\ell}^{(1)} = [\min\{\beta_{2,\ell}; \zeta_{2,\ell}^{(1)}\}]^+.$$

Otherwise, if $\frac{w_2}{w_0} \leq \frac{h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, then

$$p_{0,\ell}^{(1)} = [\gamma_\ell^{(1)}]^+ \quad \text{and} \quad p_{2,\ell}^{(1)} = 0 \quad (14)$$

where λ is chosen to satisfy the total power constraint (4).

(P2) For $\ell \in S_1$, if $\frac{w_1}{w_0} > \frac{h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, then

$$p_{0,\ell}^{(2)} = [\eta_\ell^{(2)} - \kappa_{1,\ell}^{(2)}]^+ \quad \text{and} \quad p_{1,\ell}^{(2)} = [\min\{\beta_{1,\ell}; \kappa_{1,\ell}^{(2)}\}]^+.$$

Otherwise, if $\frac{w_1}{w_0} \leq \frac{h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, then

$$p_{0,\ell}^{(2)} = [\eta_\ell^{(2)}]^+ \quad \text{and} \quad p_{1,\ell}^{(2)} = 0.$$

For $\ell \in S_2$, if $\frac{w_2}{w_0} > \frac{h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, then

$$p_{0,\ell}^{(2)} = [\eta_\ell^{(2)} - \kappa_{2,\ell}^{(2)}]^+ \quad \text{and} \quad p_{2,\ell}^{(2)} = [\min\{\beta_{2,\ell}; \kappa_{2,\ell}^{(2)}\}]^+.$$

Otherwise, if $\frac{w_2}{w_0} \leq \frac{h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, then

$$p_{0,\ell}^{(2)} = [\eta_\ell^{(2)}]^+ \quad \text{and} \quad p_{2,\ell}^{(2)} = 0 \quad (15)$$

where λ is chosen to satisfy the total power constraint (4).

(P3) For $\ell \in S_1$, if $\frac{w_1}{w_0} > \frac{\alpha h_{1,\ell}^2 + (1-\alpha)h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, then

$$p_{0,\ell}^{(3)} = [\nu_\ell^{(3)} - \xi_{1,\ell}^{(3)}]^+ \quad \text{and} \quad p_{1,\ell}^{(3)} = [\min\{\beta_{1,\ell}; \xi_{1,\ell}^{(3)}\}]^+.$$

Otherwise, if $\frac{w_1}{w_0} \leq \frac{\alpha h_{1,\ell}^2 + (1-\alpha)h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, then

$$p_{0,\ell}^{(3)} = [\nu_\ell^{(3)}]^+ \quad \text{and} \quad p_{1,\ell}^{(3)} = 0.$$

For $\ell \in S_2$, if $\frac{w_2}{w_0} > \frac{\alpha h_{1,\ell}^2 + (1-\alpha)h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, then

$$p_{0,\ell}^{(3)} = \left[\nu_\ell^{(3)} - \xi_{2,\ell}^{(3)} \right]^+ \quad \text{and} \quad p_{2,\ell}^{(3)} = \left[\min \left\{ \beta_{2,\ell}; \xi_{2,\ell}^{(3)} \right\} \right]^+.$$

Otherwise, if $\frac{w_2}{w_0} \leq \frac{\alpha h_{1,\ell}^2 + (1-\alpha)h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, then

$$p_{0,\ell}^{(3)} = \left[\nu_\ell^{(3)} \right]^+ \quad \text{and} \quad p_{2,\ell}^{(3)} = 0 \quad (16)$$

where λ is chosen to satisfy the total power constraint (4), and α is chosen to satisfy $R_{01}^{\max}(\mathbf{p}^{(3)}) = R_{02}^{\max}(\mathbf{p}^{(3)})$.

Proof: See the Appendix. ■

Based on Theorem 1, we provide the optimal power allocation algorithm that solves (11).

Algorithm that solves (11)

Step 1 Compute $\mathbf{p}^{(1)}$ by (14).

If $R_{01}^{\max}(\mathbf{p}^{(1)}) < R_{02}^{\max}(\mathbf{p}^{(1)})$, then $\mathbf{p}^* = \mathbf{p}^{(1)}$.

Otherwise, go to *Step 2*.

Step 2 Compute $\mathbf{p}^{(2)}$ by (15).

If $R_{01}^{\max}(\mathbf{p}^{(2)}) > R_{02}^{\max}(\mathbf{p}^{(2)})$, then $\mathbf{p}^* = \mathbf{p}^{(2)}$.

Otherwise, go to *Step 3*.

Step 3 Compute $\mathbf{p}^{(3)}$ by (16).

Then $\mathbf{p}^* = \mathbf{p}^{(3)}$.

IV. NUMERICAL RESULTS

In this section, we validate the analytical results by considering a system where the number of sub-channels L and the total power P are both fixed to 64. Each sub-channel is Rayleigh fading with a coefficient that remains constant for the entire transmission. Thus, the powers of the channel gains $h_{1,\ell}^2$ and $h_{2,\ell}^2$ are exponentially distributed with means $\text{SNR}_1 = \mathbb{E}\{h_{1,\ell}^2\}$ and $\text{SNR}_2 = \mathbb{E}\{h_{2,\ell}^2\}$.

Fig. 2 shows a contour plot of the boundary surface for the three dimensional secrecy capacity with $\text{SNR}_1 = \text{SNR}_2 = 10$ dB. We remark that the surface of the secrecy capacity region gets smaller as R_0 increases. Moreover, the secrecy capacity region is symmetric for the same average SNR values of both users.

Fig. 3 shows the average message information rates R_0 , R_1 and R_2 versus SNR_2 obtained by \mathbf{p}^* when $w_0 = w_1 = w_2 = 1$, while SNR_1 is fixed to 10 dB. When comparing R_1 and R_2 , we observe as expected that the two curves cross at $\text{SNR}_2 = 10$ dB before R_2 becoming higher for $\text{SNR}_2 > 10$ dB. The common message information rate R_0 increases rapidly for $\text{SNR}_2 < 10$ dB and slowly for $\text{SNR}_2 > 10$ dB. Actually, R_0 is given by the minimum of information rates between users 1 and 2. As SNR_1 is fixed to 10 dB, R_0 increases slowly for $\text{SNR}_2 > 10$ dB until reaching a floor.

Finally, we compare the performance of our algorithm with two other schemes. The first one is uniform power allocation over the sub-channels and over the three messages. The second scheme is the power allocation algorithm proposed in [18] which maximizes the sum secrecy-rate in the presence of

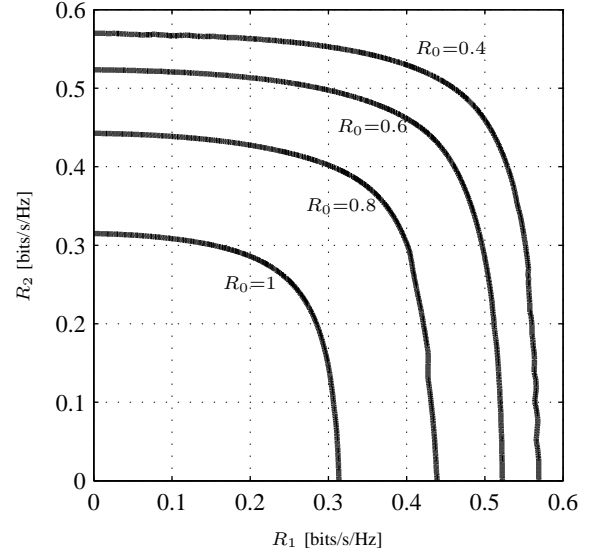


Fig. 2. Contour plot of the boundary surface of the secrecy capacity region.

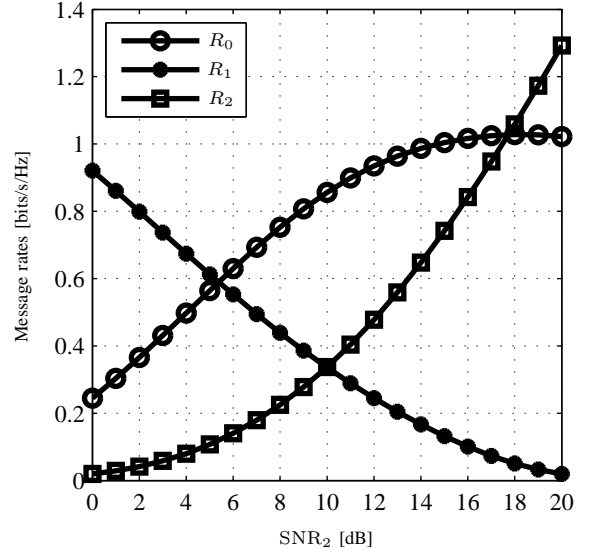


Fig. 3. Comparison of message information rates with $w_0 = w_1 = w_2 = 1$ versus SNR_2 .

two confidential messages but without a common message. In order to compare with [18] in our scenario, we first assign power $P/3$ to transmit the common message and then we split the remaining power $2 \times P/3$ between the two confidential messages according to the algorithm of [18]. Fig. 4 compares the sum-rate ($R_0 + R_1 + R_2$) of our algorithm with the two schemes versus $\text{SNR} = \text{SNR}_1 = \text{SNR}_2$. The optimal algorithm provides a significant advantage mainly at high SNR range.

V. CONCLUSIONS

The characterization of the boundary for the secrecy capacity region of an OFDM multicarrier broadcast communication yields to study a power allocation optimization problem. We are able to solve the optimization problem analytically and

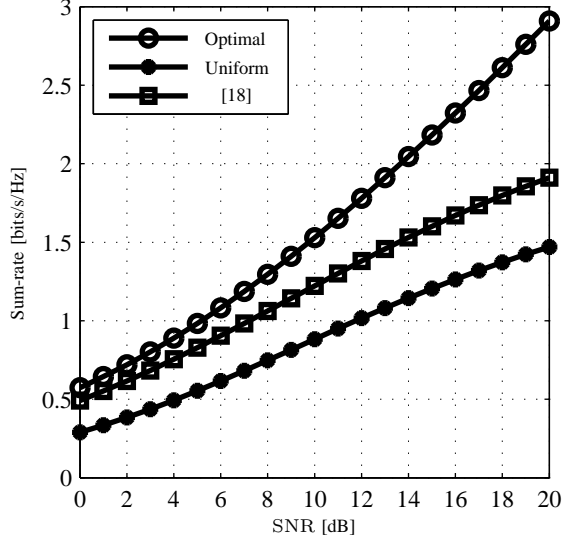


Fig. 4. Comparison of sum-rate between some power allocation algorithms versus SNR.

thus we derive the optimal power allocation algorithm. Numerical simulations validate the theoretical results. Furthermore, comparison with existing power allocation schemes highlights the significant advantage of the optimal algorithm. Future work will investigate the generalization to a number of users $K > 2$.

APPENDIX PROOF OF THEOREM 1

The interested reader can consult [21] for the proof of Lemma 1. We focus on the proof of Theorem 1. For each problem (P1)-(P3), we solve the optimization problem by a technique developed in [22] and used in [10]. The principle is based on deriving an upper bound on the Lagrangian operator and establishing power allocations that achieve the upper bound.

(P1) The Lagrangian \mathcal{L} of (P1) is given by

$$\begin{aligned} \mathcal{L} = & \sum_{\ell=1}^L \frac{w_0}{2} \log\left(1 + \frac{h_{1,\ell}^2 p_{0,\ell}}{1 + h_{1,\ell}^2 [p_{1,\ell} + p_{2,\ell}]}\right) \\ & + \sum_{\ell \in S_1} \frac{w_1}{2} \log(1 + h_{1,\ell}^2 p_{1,\ell}) - \frac{w_1}{2} \log(1 + h_{2,\ell}^2 p_{1,\ell}) \\ & + \sum_{\ell \in S_2} \frac{w_2}{2} \log(1 + h_{2,\ell}^2 p_{2,\ell}) - \frac{w_2}{2} \log(1 + h_{1,\ell}^2 p_{2,\ell}) \\ & - \lambda \sum_{\ell=1}^L [p_{0,\ell} + p_{1,\ell} + p_{2,\ell}] \end{aligned} \quad (17)$$

where $\lambda \geq 0$ is the Lagrange multiplier. For $\ell \in S_1$, the transmitter merely sends the common message and the confidential message M_1 (i.e., $p_{1,\ell} = 0$). While for $\ell \in S_2$, we have $p_{1,\ell} = 0$.

For $\ell \in S_1$, $p_{0,\ell}^{(1)}$ and $p_{1,\ell}^{(1)}$ need to maximize the following

Lagrangian \mathcal{L}_1 :

$$\begin{aligned} \mathcal{L}_1 = & \frac{w_0}{2} \log\left(1 + \frac{h_{1,\ell}^2 p_{0,\ell}}{1 + h_{1,\ell}^2 p_{1,\ell}}\right) + \frac{w_1}{2} \log(1 + h_{1,\ell}^2 p_{1,\ell}) \\ & - \frac{w_1}{2} \log(1 + h_{2,\ell}^2 p_{1,\ell}) - \lambda(p_{0,\ell} + p_{1,\ell}). \end{aligned} \quad (18)$$

We define:

$$u_{0,\ell}^{(1)}(x) = \frac{w_0}{2 \ln 2} \frac{h_{1,\ell}^2}{1 + h_{1,\ell}^2 x} - \lambda \quad (19)$$

$$u_{1,\ell}(x) = \frac{w_1}{2 \ln 2} \left(\frac{h_{1,\ell}^2}{1 + h_{1,\ell}^2 x} - \frac{h_{2,\ell}^2}{1 + h_{2,\ell}^2 x} \right) - \lambda. \quad (20)$$

Then,

$$\begin{aligned} \mathcal{L}_1 &= \int_{p_{1,\ell}}^{p_{1,\ell} + p_{0,\ell}} u_{0,\ell}^{(1)}(x) dx + \int_0^{p_{1,\ell}} u_{1,\ell}(x) dx \\ &\leq \int_0^{+\infty} [\max\{u_{0,\ell}^{(1)}(x), u_{1,\ell}(x)\}]^+ dx. \end{aligned} \quad (21)$$

The root of $u_{0,\ell}^{(1)}(x)$ is $\gamma_\ell^{(1)}$ defined in (13b) while the largest root of $u_{1,\ell}(x)$ is $\beta_{1,\ell}$ defined in (13a). $u_{0,\ell}^{(1)}(x)$ and $u_{1,\ell}(x)$ intersect at the point $\zeta_{1,\ell}^{(1)}$ given by (13c). In the following, we consider two cases.

- 1) $\frac{w_1}{w_0} > \frac{h_{1,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, i.e., $\zeta_{1,\ell}^{(1)}$ is positive.

In this case, $u_{1,\ell}(0) > u_{0,\ell}^{(1)}(0)$. There are three possibilities to consider depending on the value of λ .

- a) If $u_{1,\ell}(0) < 0$, then both $u_{0,\ell}^{(1)}(x)$ and $u_{1,\ell}(x)$ are negative for $x > 0$. The upper bound on \mathcal{L}_1 in (21) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{1,\ell}^{(1)} = 0$.
- b) If $u_{1,\ell}(0) \geq 0$ and $\gamma_\ell^{(1)} < \zeta_{1,\ell}^{(1)}$, then the upper bound on \mathcal{L}_1 in (21) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{1,\ell}^{(1)} = \beta_{1,\ell}$.
- c) If $\gamma_\ell^{(1)} \geq \zeta_{1,\ell}^{(1)}$, then the upper bound on \mathcal{L}_1 in (21) is achieved by $p_{0,\ell}^{(1)} = \gamma_\ell^{(1)} - \zeta_{1,\ell}^{(1)}$ and $p_{1,\ell}^{(1)} = \zeta_{1,\ell}^{(1)}$.

In summary, we obtain

$$p_{0,\ell}^{(1)} = [\gamma_\ell^{(1)} - \zeta_{1,\ell}^{(1)}]^+ \text{ and } p_{1,\ell}^{(1)} = [\min\{\beta_{1,\ell}, \zeta_{1,\ell}^{(1)}\}]^+. \quad (22)$$

- 2) $\frac{w_1}{w_0} \leq \frac{h_{1,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, i.e., $\zeta_{1,\ell}^{(1)}$ is negative.

In this case, $u_{0,\ell}^{(1)}(0) \geq u_{1,\ell}(0)$.

- a) If $u_{0,\ell}^{(1)}(0) \leq 0$, then the upper bound on \mathcal{L}_1 in (21) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{1,\ell}^{(1)} = 0$.
- b) If $u_{0,\ell}^{(1)}(0) > 0$, then the upper bound on \mathcal{L}_1 in (21) is achieved by $p_{0,\ell}^{(1)} = \gamma_\ell^{(1)}$ and $p_{1,\ell}^{(1)} = 0$.

In summary,

$$p_{0,\ell}^{(1)} = [\gamma_\ell^{(1)}]^+ \text{ and } p_{1,\ell}^{(1)} = 0. \quad (23)$$

For $\ell \in S_2$, $p_{0,\ell}^{(1)}$ and $p_{2,\ell}^{(1)}$ need to maximize the following Lagrangian \mathcal{L}_2 :

$$\mathcal{L}_2 = \frac{w_0}{2} \log\left(1 + \frac{h_{1,\ell}^2 p_{0,\ell}}{1 + h_{1,\ell}^2 p_{2,\ell}}\right) + \frac{w_2}{2} \log(1 + h_{2,\ell}^2 p_{2,\ell}) - \frac{w_2}{2} \log(1 + h_{1,\ell}^2 p_{2,\ell}) - \lambda(p_{0,\ell} + p_{2,\ell}). \quad (24)$$

We define:

$$u_{2,\ell}(x) = \frac{w_2}{2 \ln 2} \left(\frac{h_{2,\ell}^2}{1 + h_{2,\ell}^2 x} - \frac{h_{1,\ell}^2}{1 + h_{1,\ell}^2 x} \right) - \lambda. \quad (25)$$

Then,

$$\begin{aligned} \mathcal{L}_2 &= \int_{p_{2,\ell}}^{p_{2,\ell} + p_{0,\ell}} u_{0,\ell}^{(1)}(x) dx + \int_0^{p_{2,\ell}} u_{2,\ell}(x) dx \\ &\leq \int_0^{+\infty} \left[\max\{u_{0,\ell}^{(1)}(x), u_{2,\ell}(x)\} \right]^+ dx. \end{aligned} \quad (26)$$

The largest root of $u_{2,\ell}(x)$ is $\beta_{2,\ell}$ given by (13a). Moreover, $u_{0,\ell}^{(1)}(x)$ and $u_{2,\ell}(x)$ intersect at the point $\zeta_{2,\ell}^{(1)}$ given by (13c). We consider two cases depending on the sign of $\zeta_{2,\ell}^{(1)}$.

- 1) $\frac{w_2}{w_0} > \frac{h_{1,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, i.e., $\zeta_{2,\ell}^{(1)}$ is positive.

In this case, $u_{2,\ell}(0) > u_{0,\ell}^{(1)}(0)$. There are three possibilities to consider.

- If $u_{2,\ell}(0) < 0$, then both $u_{0,\ell}^{(1)}(x)$ and $u_{2,\ell}(x)$ are negative for $x > 0$. The upper bound on \mathcal{L}_2 in (26) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{2,\ell}^{(1)} = 0$.
- If $u_{2,\ell}(0) \geq 0$ and $\gamma_\ell^{(1)} < \zeta_{2,\ell}^{(1)}$, then the upper bound on \mathcal{L}_2 in (26) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{2,\ell}^{(1)} = \beta_{2,\ell}$.
- If $\gamma_\ell^{(1)} \geq \zeta_{2,\ell}^{(1)}$, then the upper bound on \mathcal{L}_2 in (26) is achieved by $p_{0,\ell}^{(1)} = \gamma_\ell^{(1)} - \zeta_{2,\ell}^{(1)}$ and $p_{2,\ell}^{(1)} = \zeta_{2,\ell}^{(1)}$.

In summary, we have

$$p_{0,\ell}^{(1)} = \left[\gamma_\ell^{(1)} - \zeta_{2,\ell}^{(1)} \right]^+ \text{ and } p_{2,\ell}^{(1)} = \left[\min\{\beta_{2,\ell}; \zeta_{2,\ell}^{(1)}\} \right]^+. \quad (27)$$

- 2) $\frac{w_2}{w_0} \leq \frac{h_{1,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, i.e., $\zeta_{2,\ell}^{(1)}$ is negative.

In this case, $u_{0,\ell}^{(1)}(0) \geq u_{2,\ell}(0)$. There are two possibilities to consider.

- If $u_{0,\ell}^{(1)}(0) \leq 0$, then the upper bound on \mathcal{L}_2 in (26) is achieved by $p_{0,\ell}^{(1)} = 0$ and $p_{2,\ell}^{(1)} = 0$.
- If $u_{0,\ell}^{(1)}(0) > 0$, then the upper bound on \mathcal{L}_2 in (26) is achieved by $p_{0,\ell}^{(1)} = \gamma_\ell^{(1)}$ and $p_{2,\ell}^{(1)} = 0$.

In summary,

$$p_{0,\ell}^{(1)} = \left[\gamma_\ell^{(1)} \right]^+ \text{ and } p_{2,\ell}^{(1)} = 0. \quad (28)$$

The Lagrange parameter λ is chosen to satisfy the power constraint.

(P2) The Lagrangian of (P2) is given by

$$\begin{aligned} \mathcal{L} &= \sum_{\ell=1}^L \frac{w_0}{2} \log\left(1 + \frac{h_{2,\ell}^2 p_{0,\ell}}{1 + h_{2,\ell}^2 [p_{1,\ell} + p_{2,\ell}]}\right) \\ &\quad + \sum_{\ell \in S_1} \frac{w_1}{2} \log(1 + h_{1,\ell}^2 p_{1,\ell}) - \frac{w_1}{2} \log(1 + h_{2,\ell}^2 p_{1,\ell}) \\ &\quad + \sum_{\ell \in S_2} \frac{w_2}{2} \log(1 + h_{2,\ell}^2 p_{2,\ell}) - \frac{w_2}{2} \log(1 + h_{1,\ell}^2 p_{2,\ell}) \\ &\quad - \lambda \sum_{\ell=1}^L [p_{0,\ell} + p_{1,\ell} + p_{2,\ell}] \end{aligned} \quad (29)$$

where $\lambda \geq 0$ is the Lagrange multiplier.

For $\ell \in S_1$, $p_{0,\ell}^{(2)}$ and $p_{1,\ell}^{(2)}$ need to maximize the following Lagrangian \mathcal{L}_1 :

$$\begin{aligned} \mathcal{L}_1 &= \frac{w_0}{2} \log\left(1 + \frac{h_{2,\ell}^2 p_{0,\ell}}{1 + h_{2,\ell}^2 p_{1,\ell}}\right) + \frac{w_1}{2} \log(1 + h_{1,\ell}^2 p_{1,\ell}) \\ &\quad - \frac{w_1}{2} \log(1 + h_{2,\ell}^2 p_{1,\ell}) - \lambda(p_{0,\ell} + p_{1,\ell}). \end{aligned} \quad (30)$$

We define:

$$u_{0,\ell}^{(2)}(x) = \frac{w_0}{2 \ln 2} \frac{h_{2,\ell}^2}{1 + h_{2,\ell}^2 x} - \lambda. \quad (31)$$

Then,

$$\begin{aligned} \mathcal{L}_1 &= \int_{p_{1,\ell}}^{p_{1,\ell} + p_{0,\ell}} u_{0,\ell}^{(2)}(x) dx + \int_0^{p_{1,\ell}} u_{1,\ell}(x) dx \\ &\leq \int_0^{+\infty} \left[\max\{u_{0,\ell}^{(2)}(x), u_{1,\ell}(x)\} \right]^+ dx. \end{aligned} \quad (32)$$

The root of $u_{0,\ell}^{(2)}(x)$ is $\eta_\ell^{(2)}$ given by (13d). Furthermore, $u_{0,\ell}^{(2)}(x)$ and $u_{1,\ell}(x)$ intersect at the point $\kappa_{1,\ell}^{(2)}$ given by (13e). Following similar steps as (P1), we consider two cases.

- 1) $\frac{w_1}{w_0} > \frac{h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, i.e., $\kappa_{1,\ell}^{(2)}$ is positive. Then,

$$p_{0,\ell}^{(2)} = \left[\eta_\ell^{(2)} - \kappa_{1,\ell}^{(2)} \right]^+ \text{ and } p_{1,\ell}^{(2)} = \left[\min\{\beta_{1,\ell}; \kappa_{1,\ell}^{(2)}\} \right]^+. \quad (33)$$

- 2) $\frac{w_1}{w_0} \leq \frac{h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, i.e., $\kappa_{1,\ell}^{(2)}$ is negative. Then,

$$p_{0,\ell}^{(2)} = \left[\eta_\ell^{(2)} \right]^+ \text{ and } p_{1,\ell}^{(2)} = 0. \quad (34)$$

For $\ell \in S_2$, $p_{0,\ell}^{(2)}$ and $p_{2,\ell}^{(2)}$ need to maximize the following Lagrangian \mathcal{L}_2 :

$$\begin{aligned} \mathcal{L}_2 &= \frac{w_0}{2} \log\left(1 + \frac{h_{2,\ell}^2 p_{0,\ell}}{1 + h_{2,\ell}^2 p_{2,\ell}}\right) + \frac{w_2}{2} \log(1 + h_{2,\ell}^2 p_{2,\ell}) \\ &\quad - \frac{w_2}{2} \log(1 + h_{1,\ell}^2 p_{2,\ell}) - \lambda(p_{0,\ell} + p_{2,\ell}). \end{aligned} \quad (35)$$

Then,

$$\begin{aligned} \mathcal{L}_2 &= \int_{p_{2,\ell}}^{p_{2,\ell} + p_{0,\ell}} u_{0,\ell}^{(2)}(x) dx + \int_0^{p_{2,\ell}} u_{2,\ell}(x) dx \\ &\leq \int_0^{+\infty} \left[\max\{u_{0,\ell}^{(2)}(x), u_{2,\ell}(x)\} \right]^+ dx. \end{aligned} \quad (36)$$

$u_{0,\ell}^{(2)}(x)$ and $u_{2,\ell}(x)$ intersect at the point $\kappa_{2,\ell}^{(2)}$ given by (13e). Depending on the sign of $\kappa_{2,\ell}^{(2)}$, we consider two cases.

1) $\frac{w_2}{w_0} > \frac{h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, i.e., $\kappa_{2,\ell}^{(2)}$ is positive. Then,

$$p_{0,\ell}^{(2)} = \left[\eta_\ell^{(2)} - \kappa_{2,\ell}^{(2)} \right]^+ \text{ and } p_{2,\ell}^{(2)} = \left[\min\{\beta_{2,\ell}; \kappa_{2,\ell}^{(2)}\} \right]^+. \quad (37)$$

2) $\frac{w_2}{w_0} \leq \frac{h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, i.e., $\kappa_{2,\ell}^{(2)}$ is negative. Then,

$$p_{0,\ell}^{(2)} = \left[\eta_\ell^{(2)} \right]^+ \text{ and } p_{2,\ell}^{(2)} = 0. \quad (38)$$

(P3) The Lagrangian of (P3) is

$$\begin{aligned} \mathcal{L} = & \sum_{\ell=1}^L \frac{w_0 \alpha}{2} \log\left(1 + \frac{h_{1,\ell}^2 p_{0,\ell}}{1 + h_{1,\ell}^2 [p_{1,\ell} + p_{2,\ell}]}\right) \\ & + \frac{w_0(1-\alpha)}{2} \log\left(1 + \frac{h_{2,\ell}^2 p_{0,\ell}}{1 + h_{2,\ell}^2 [p_{1,\ell} + p_{2,\ell}]}\right) \\ & + \sum_{\ell \in S_1} \frac{w_1}{2} \log(1 + h_{1,\ell}^2 p_{1,\ell}) - \frac{w_1}{2} \log(1 + h_{2,\ell}^2 p_{1,\ell}) \\ & + \sum_{\ell \in S_2} \frac{w_2}{2} \log(1 + h_{2,\ell}^2 p_{2,\ell}) - \frac{w_2}{2} \log(1 + h_{1,\ell}^2 p_{2,\ell}) \\ & - \lambda \sum_{\ell=1}^L [p_{0,\ell} + p_{1,\ell} + p_{2,\ell}] \end{aligned} \quad (39)$$

where $\lambda \geq 0$ is the Lagrange multiplier.

For $\ell \in S_1$, $p_{0,\ell}^{(3)}$ and $p_{1,\ell}^{(3)}$ need to maximize the following Lagrangian \mathcal{L}_1 :

$$\begin{aligned} \mathcal{L}_1 = & \frac{w_0 \alpha}{2} \log\left(1 + \frac{h_{1,\ell}^2 p_{0,\ell}}{1 + h_{1,\ell}^2 p_{1,\ell}}\right) \\ & + \frac{w_0(1-\alpha)}{2} \log\left(1 + \frac{h_{2,\ell}^2 p_{0,\ell}}{1 + h_{2,\ell}^2 p_{1,\ell}}\right) \\ & + \frac{w_1}{2} \log(1 + h_{1,\ell}^2 p_{1,\ell}) - \frac{w_1}{2} \log(1 + h_{2,\ell}^2 p_{1,\ell}) \\ & - \lambda(p_{0,\ell} + p_{1,\ell}). \end{aligned} \quad (40)$$

We define:

$$u_{0,\ell}^{(3)}(x) = \frac{w_0}{2 \ln 2} \left(\frac{\alpha h_{1,\ell}^2}{1 + h_{1,\ell}^2 x} + \frac{(1-\alpha) h_{2,\ell}^2}{1 + h_{2,\ell}^2 x} \right) - \lambda. \quad (41)$$

Then,

$$\begin{aligned} \mathcal{L}_1 &= \int_{p_{1,\ell}}^{p_{1,\ell} + p_{0,\ell}} u_{0,\ell}^{(3)}(x) dx + \int_0^{p_{1,\ell}} u_{1,\ell}(x) dx \\ &\leq \int_0^{+\infty} \left[\max\{u_{0,\ell}^{(3)}(x); u_{1,\ell}(x)\} \right]^+ dx. \end{aligned} \quad (42)$$

The largest root of $u_{0,\ell}^{(3)}(x)$ is $\nu_\ell^{(3)}$ given by (13f). Furthermore, $u_{0,\ell}^{(3)}(x)$ and $u_{1,\ell}(x)$ intersect at the point $\xi_{1,\ell}^{(3)}$ given by (13g). Following similar steps as (P1), we consider two cases.

1) $\frac{w_1}{w_0} > \frac{\alpha h_{1,\ell}^2 + (1-\alpha) h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, i.e., $\xi_{1,\ell}^{(3)}$ is positive. Then,

$$p_{0,\ell}^{(3)} = \left[\nu_\ell^{(3)} - \xi_{1,\ell}^{(3)} \right]^+ \text{ and } p_{1,\ell}^{(3)} = \left[\min\{\beta_{1,\ell}; \xi_{1,\ell}^{(3)}\} \right]^+. \quad (43)$$

2) $\frac{w_1}{w_0} \leq \frac{\alpha h_{1,\ell}^2 + (1-\alpha) h_{2,\ell}^2}{h_{1,\ell}^2 - h_{2,\ell}^2}$, i.e., $\xi_{1,\ell}^{(3)}$ is negative. Then,

$$p_{0,\ell}^{(3)} = \left[\nu_\ell^{(3)} \right]^+ \text{ and } p_{1,\ell}^{(3)} = 0. \quad (44)$$

For $\ell \in S_2$, $p_{0,\ell}^{(3)}$ and $p_{2,\ell}^{(3)}$ need to maximize the following Lagrangian \mathcal{L}_2 :

$$\begin{aligned} \mathcal{L}_2 = & \frac{w_0 \alpha}{2} \log\left(1 + \frac{h_{1,\ell}^2 p_{0,\ell}}{1 + h_{1,\ell}^2 p_{2,\ell}}\right) \\ & + \frac{w_0(1-\alpha)}{2} \log\left(1 + \frac{h_{2,\ell}^2 p_{0,\ell}}{1 + h_{2,\ell}^2 p_{2,\ell}}\right) \\ & + \frac{w_2}{2} \log(1 + h_{2,\ell}^2 p_{2,\ell}) - \frac{w_2}{2} \log(1 + h_{1,\ell}^2 p_{2,\ell}) \\ & - \lambda(p_{0,\ell} + p_{2,\ell}). \end{aligned} \quad (45)$$

The operator \mathcal{L}_2 can be upper bounded by:

$$\begin{aligned} \mathcal{L}_2 &= \int_{p_{2,\ell}}^{p_{2,\ell} + p_{0,\ell}} u_{0,\ell}^{(3)}(x) dx + \int_0^{p_{2,\ell}} u_{2,\ell}(x) dx \\ &\leq \int_0^{+\infty} \left[\max\{u_{0,\ell}^{(3)}(x); u_{2,\ell}(x)\} \right]^+ dx. \end{aligned} \quad (46)$$

$u_{0,\ell}^{(3)}(x)$ and $u_{2,\ell}(x)$ intersect at the point $\xi_{2,\ell}^{(3)}$. Following similar steps as (P1), we consider two cases.

1) $\frac{w_2}{w_0} > \frac{\alpha h_{1,\ell}^2 + (1-\alpha) h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, i.e., $\xi_{2,\ell}^{(3)}$ is positive. Then,

$$p_{0,\ell}^{(3)} = \left[\nu_\ell^{(3)} - \xi_{2,\ell}^{(3)} \right]^+ \text{ and } p_{2,\ell}^{(3)} = \left[\min\{\beta_{2,\ell}; \xi_{2,\ell}^{(3)}\} \right]^+. \quad (47)$$

2) $\frac{w_2}{w_0} \leq \frac{\alpha h_{1,\ell}^2 + (1-\alpha) h_{2,\ell}^2}{h_{2,\ell}^2 - h_{1,\ell}^2}$, i.e., $\xi_{2,\ell}^{(3)}$ is negative. Then,

$$p_{0,\ell}^{(3)} = \left[\nu_\ell^{(3)} \right]^+ \text{ and } p_{2,\ell}^{(3)} = 0. \quad (48)$$

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Inter. Symp. Inf. Theory*, Seattle, WA, USA, July 2006, pp. 356–360.
- [3] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *IEEE Inter. Symp. Inf. Theory*, Nice, France, June 2007, pp. 1296–1300.
- [4] P. K. Gopala, L. Lai, and H. ElGamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.
- [6] —, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [8] A. Mukherjee, S. Ali., A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks," 2014, to be published.
- [9] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [10] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

- [11] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.
- [12] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.
- [13] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.
- [14] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.
- [15] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.
- [16] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.
- [17] —, "Secure broadcasting using multiple antennas," *Journal of Communications and Networks*, vol. 12, no. 5, pp. 411–432, Oct. 2010.
- [18] E. Jorswieck and S. Gerbracht, "Secrecy rate region of downlink OFDM systems: Efficient resource allocation," in *Proc. 14th Int. OFDM-Workshop (InOWo)*, Hamburg, Germany, Sep. 2009.
- [19] E. Ekrem and S. Ulukus, "Ergodic secrecy capacity region of the fading broadcast channel," in *IEEE Int. Conf. Commun. (ICC'09)*, Dresden, Germany, June 2009, pp. 1–5.
- [20] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.
- [21] Y. Liang, V. V. Veeravalli, and H. V. Poor, "Resource allocation for wireless fading channels: Max-min solution," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3432–3453, Oct. 2007.
- [22] D. N. C. Tse, "Optimal power allocation over parallel Gaussian broadcast channels," in *IEEE Int. Symp. Inf. Theory*, Ulm, Germany, June 1997, p. 27.